FortiAuthenticator™ 4.0
What's New Guide

FortiAuthenticator™ 4.0 What's New Guide

July 29, 2015

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2015-07-28	Initial Release

Introduction

This document lists and describes many of the new features added to FortiAuthenticator™ 4.0. For a complete list of all new FortiAuthenticator™ 4.0 features and bug fixes, please see the latest release notes.

This document, and all of the FortiAuthenticator™ 4.0 documentation, will continue to improve as we see the new features in action and as we get feedback about these documents from you. You can send comments and suggestions for improvements for all FortiAuthenticator™ 4.0 documents to techdoc@fortinet.com.

What's New

FortiAuthenticator™ 4.0 is a major feature release and includes new features in all functional areas of the product. There is a particular focus on enhancement of the Guest and Social authentication capability.

System features

These are features related to general system operation and not a specific functional area.

SNMP enhancements

Several new statistics have been added to the SNMP Agent:

facHaCurrentStatus: The current HA status of the FortiAuthenticator

facRadiusProxyInTotal: The total number of RADIUS accounting proxy packets received

facRadiusProxyOutTotal: The total number of RADIUS accounting proxy packets sent

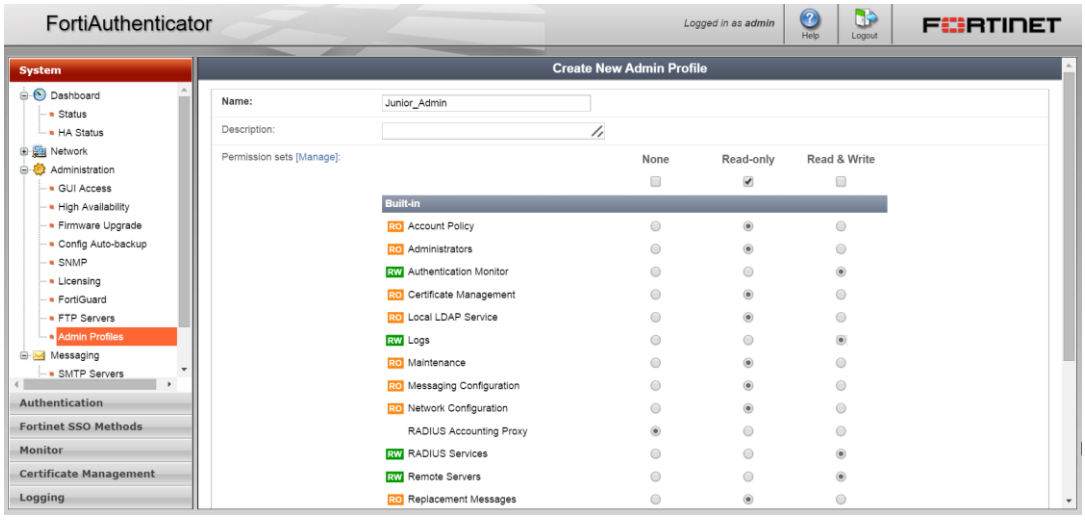
Additionally, the new trap **facTrapHAStatusChange** has been added which is triggered when there is a change in the HA status of the FortiAuthenticator.

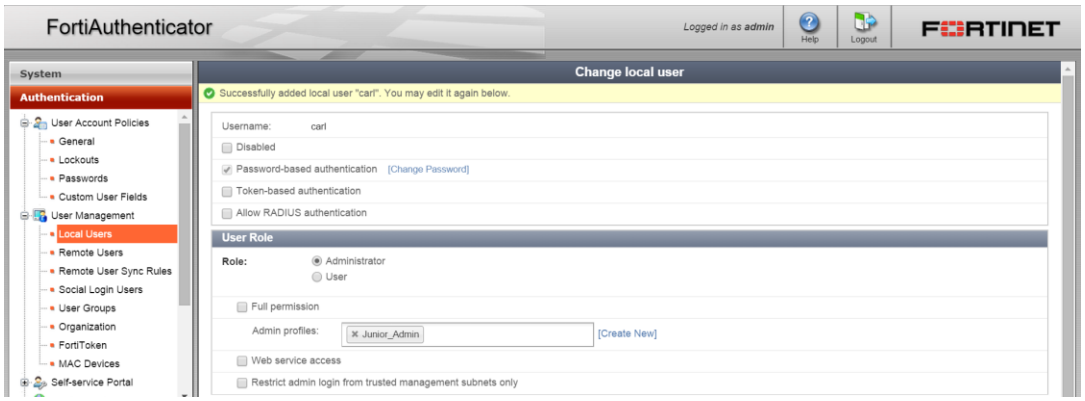
Add Riverbed RADIUS VSAs

The Riverbed RADIUS dictionary has been added to the RADIUS engine to allow Riverbed vendor attributes to be used in Authentication.

Role Based Administration

Previous releases required the administrative user permissions to be applied on a per-user basis. To simplify the configuration of user permissions, the concept of Admin User Profiles has been implemented to allow a profile to be defined according to administrator role and applied across multiple users.





Authentication

Authentication covers all of the explicit authentication options within the FortiAuthenticator including RADIUS, LDAP, Two-Factor, Tokens, EAP, guest management and user self-service features.

Social and MAC address authentication

Social Wifi authentication allows FortiAuthenticator to utilize third party user identity methods to authenticate users into a wireless guest network. Supported authentication methods include:

- Google +
- Facebook
- Linkedin
- Twitter
- Form based authentication (similar to existing self-reg feature)
    - SMS based authentication
    - Email based authentication
- MAC Address authentication

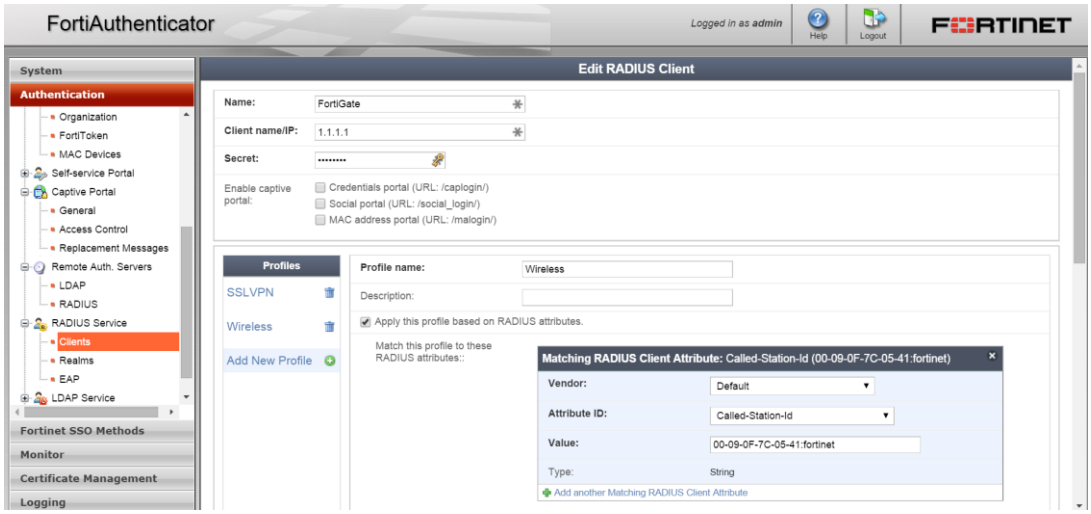
RADIUS Sub Auth Client Profiles

FortiAuthenticator previously has differentiated authentication sources based purely on IP address (NAS or RADIUS Client) and for most use cases, this is sufficient. FortiGate is somewhat unique however in that it offers multiple services on a single appliance, which may require specific configuration (groups, users, attributes, 802.1x support) for each e.g.

- Management (GUI/SSH)
- IPSEC/SSL-VPN
- Web Filtering Override
- Wireless Authentication

Each of these methods may require a different profile (permitted groups, auth methods, backend databases), yet all RADIUS authentication requests may originate from the same IP address and therefore have previously been indistinguishable to the FortiAuthenticator.

FortiAuthenticator™ 4.0 introduces the concept of RADIUS Client Profiles where the authentication profile is applied according to a RADIUS attribute in the authentication request.



Some common FortiGate RADIUS attributes which may be used to differentiate authentication profiles include:

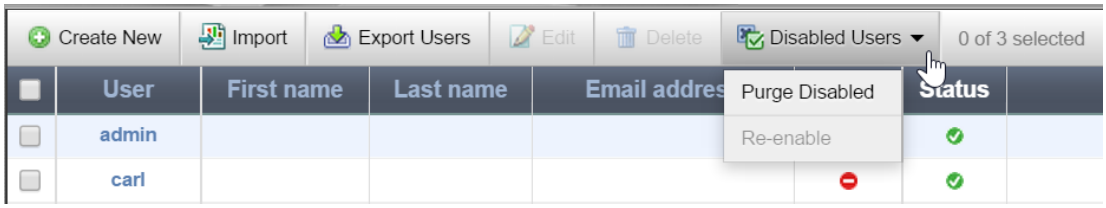
Login Type	Attribute	Value
Admin (GUI)	Connect Info attribute (77)	admin-login
Wireless 802.1X (e.g. SSID = fortinet)	NAS Port Type Attribute (61) Connect Info attribute (77) Called Station Attribute (30)	Wireless - IEEE 802.11 CONNECT 11Mbps 802.11b 00-09-0F-7C-05-41:fortinet
Captive Portal	Connect Info Attribute (77)	web-auth
SSL-VPN	Connect Info Attribute (77)	vpn-ssl
IPSEC-VPN	Connect Info Attribute (77)	vpn-ipsec

Bulk purge inactive users

The goal of this feature is to provide a convenient way to identify and manage expired user accounts.

The Local Users list page currently includes a “Status” column indicating whether the user is enabled or disabled. When the user is disabled, a comment is added specifying the reason it has been disabled (manually, expired or login inactivity).

The Local Users page has been modified to include the ability to perform a bulk disabled user purge, or re-enablement.



The “Purge Disabled” selection will offer the option to choose which type of disabled users to purge. All users matching the type(s) selection will be deleted.

The “Re-enable” selection will re-enable the selected user accounts. Note that only user accounts manually disabled or disabled because of login inactivity can be re-enabled in this fashion. Expired users accounts can only be re-enabled individually.

Active Directory password change

Previous release of FortiAuthenticator includes the ability for self-service password management for local users. FortiAuthenticator™ 4.0 extends this capability to Active Directory user password management.

Several different methods of managing the password change process are supported.

RADIUS Login

When a user authenticates via a RADIUS Client which is configured to validate the user password against a Windows AD server using MS-CHAPv2 RADIUS, a valid response from AD can be "change password". FortiAuthenticator now recognizes this response and coordinate the proper message exchange between the NAS and the Windows AD server that will result in a password change.

Note that the following conditions are required for this password change scenario to work:

- FortiAuthenticator has joined the Windows AD domain
- RADIUS client (NAS) has been configured to "Use Windows AD domain authentication"
- RADIUS authentication request uses MS-CHAPv2
- RADIUS client (NAS) must also support MS-CHAPv2 password change

GUI User Login

FortiAuthenticator also supports password change when the user performs a login via the GUI portal. If during the login process, FortiAuthenticator validates the user password against Windows AD server and the Windows AD server responds with a "change password"; the GUI will prompt the user to enter a new password.

Note that the following conditions are required for this password change scenario to work:

- FortiAuthenticator has joined the Windows AD domain

  or

- Secure LDAP is enabled and the LDAP admin (i.e. regular bind) has the permissions to reset user passwords

GUI User Portal

FortiAuthenticator also supports user initiated password change via the GUI's user portal. After successful GUI login, the user gains access to the user portal. One of the possible actions that can be initiated from the user portal is a password change.

Note that the following conditions are required for this password change scenario to work:

- FortiAuthenticator has joined the Windows AD domain

  or

- Secure LDAP is enabled and the LDAP admin (i.e. regular bind) has the permissions to reset user passwords

Allow expired FTM reactivation

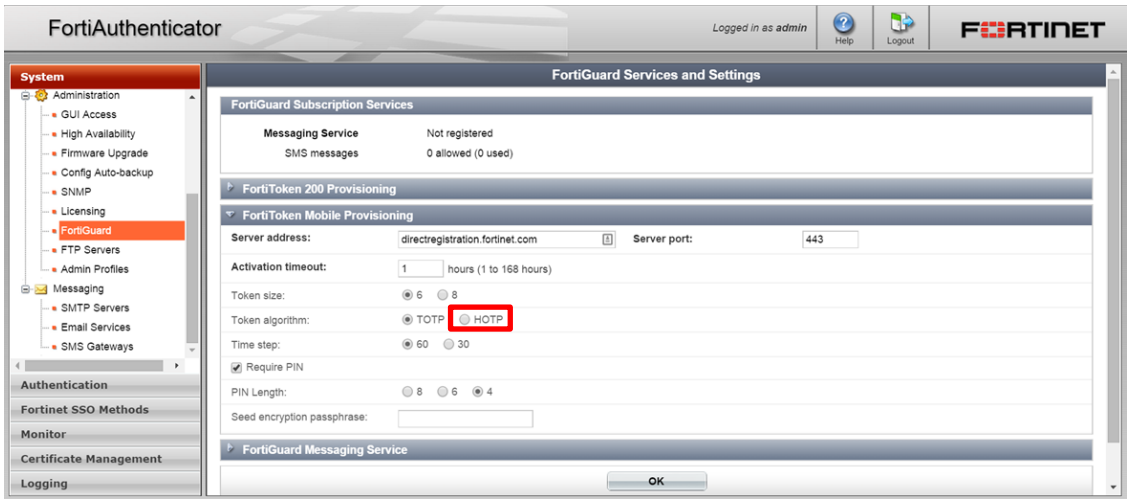
The FortiTokenMobile provisioning process is initiated when a token is associated with a user. However, the provisioning is cancelled if not completed by the end-user action before the end of a pre-configured timeout period (default 1 hour). Previously, FortiAuthenticator would put the FTM in a locked state once the timeout expired, but leave the user enabled. The user with a locked FTM would not be able to login (as expected) but was difficult for an administrator to detect, identify and rectify increasing administrator overhead.

The new workflow after the FTM provisioning period expires is now:

- Disassociate the FTM from the user
- Put the FTM back in the pool of available FTMs
- Disable the user (reason = "FTM activation timeout")

Support for FTM Event (HOTP) based tokens

The ability to provision FortiToekn Mobile Event based tokens has been added. This needs to be configured prior to the configuration of the tokens as shown.



FSSO

Fortinet Single Sign-On (FSSO) is a method used by FortiGate and FortiCache to transparently identify users on the network. FortiAuthenticator uses both transparent and non-transparent methods to gather user login status information from a variety of disparate locations; consolidates and embellishes the information before supplying to FortiGate or FortiCache devices for use in identity based policies.

DC/TS Monitor

A new monitoring page has been added to the GUI under Monitor > SSO to display information on the Domain Controller (DC) and Terminal Server (TS) agents that are reporting to the FortiAuthenticator. The monitoring page shows:

- Agent type (DC or TS)
- Name/IP address of the agent
- Last time the agent was connected to the FAC
- Agent's connection status

- Number of currently logged-on users submitted by the agent (TS agents only)

SSO filtering enhancements

Multiple changes have been made to the filtering of SSO Users to make the process more flexible and allow filtering based on User/group/OU/IP.

FortiAuthenticator collects user login information from one or more sources (Windows AD server polling, RADIUS accounting, user portal, FortiClient SSOMA, etc) and makes that information available to one or more FortiGate or FortiCache.

The login information for one user login information element consists of:

- User's IP address
- User's name
- List of groups that the user belongs to (group membership)

In most cases, the group membership information is obtained by doing a search through the user/group hierarchy of an LDAP server. In previous releases, we provided user filtering support to only include users who were members of certain usergroups on the LDAP server. In addition, we offered a way to filter out users who were within a certain IP address range.

This feature enhances the filtering mechanism to more user filtering options:

User: Specifies the DN of a user. This user must be included in SSO

Group: Specifies the DN of a group. All users who are members of that group must be included in SSO

User container: Specifies the DN of an LDAP container (e.g. OU). All users who are under that container or one of its sub-containers must be included in SSO

Group container: Specifies the DN of an LDAP container (e.g. OU). All users who members of a group under that container or one of its sub-containers must be included in SSO.

User & group container: Specifies the DN of an LDAP container (e.g. OU). It is the union of the user and the group containers.

IP: Specifies an IP range or subnet and whether users within those IP addresses must be included or excluded.

Furthermore, the above filter options will be available at two levels:

Global pre-filter: This filter is applied as the user login information as received from one of the identity sources. User login information meeting the filter requirements will be retained by the FortiAuthenticator for inclusion in the FSSO table. Other user login information is discarded.

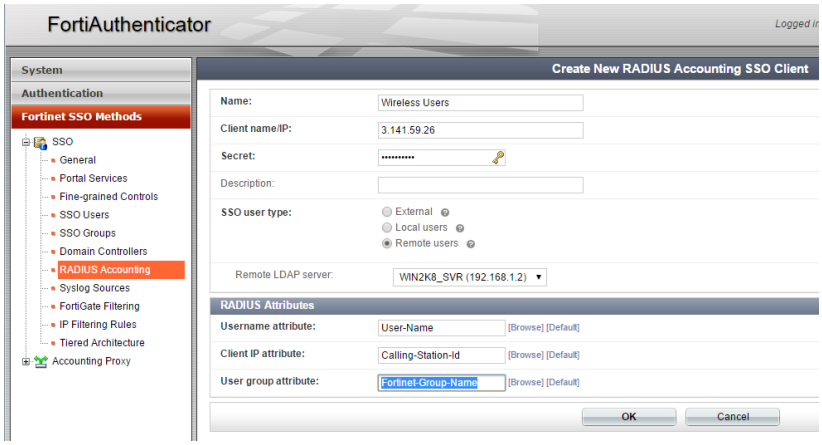
This helps to optimize performance, but also prevent overloading of the FSSO concurrent user license.

Per-FortiGate filter: This filter is applied to the user login information distributed to a specific FortiGate for scenarios where the FortiGate is only interested in a subset of the overall user login information.

RADIUS Attribute - LDAP Group mapping

When RADIUS accounting to Fortinet Single Sign-On is enabled and Remote LDAP used to pull in group information; previous release have only supported acquisition of this information from Active Directory based LDAP due to reliance on the MemberOf attribute.

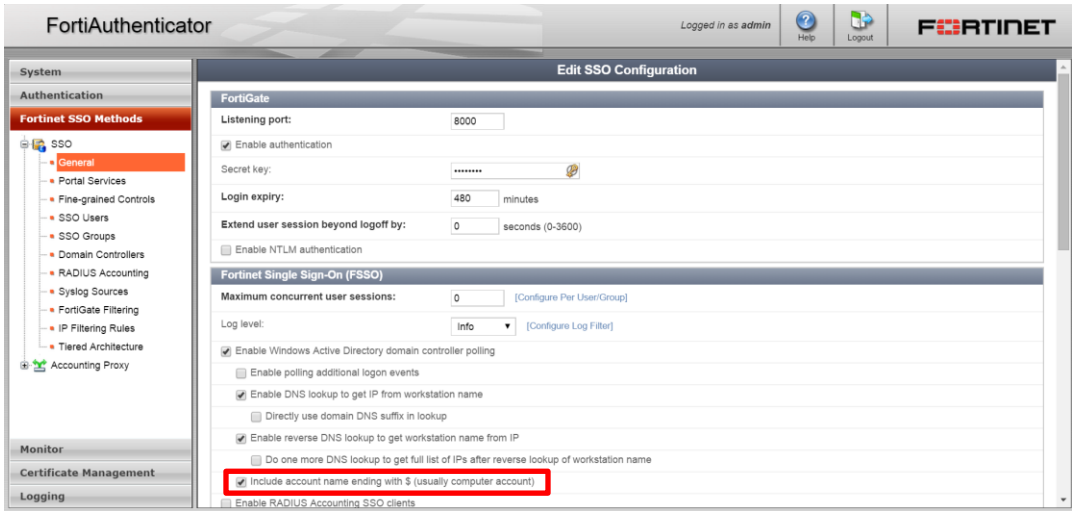
This restriction has now been removed and group information from other non-AD based LDAP directories is now also supported.



SSO - include username with '$'

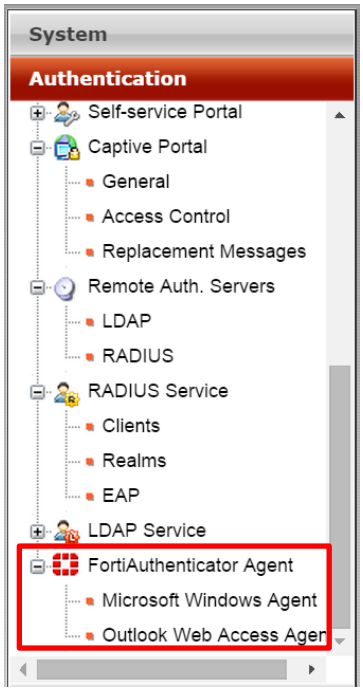
In previous firmware releases, the FortiAuthenticator excludes usernames containing the '$' character in its SSO feature since this usually indicate Computer accounts on modern versions of Windows AD servers. However, it is not a hard rule and the '$' character may still be present in usernames. It is especially more prevalent when user accounts have been migrated from older Windows NT servers.

If not relying on the '$' character to detect Computer accounts, the FortiAuthenticator must do an extra LDAP search, thus impacting performance. Therefore, we will make this feature configurable. The legacy behavior will be the default setting.



Download OWA agent from GUI

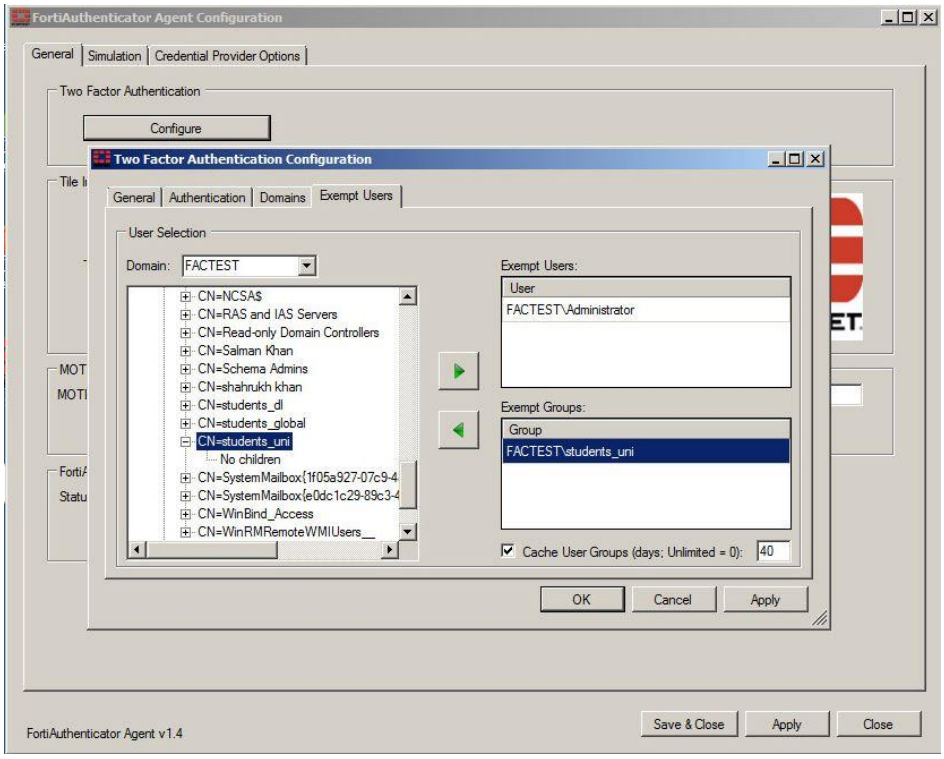
The Agent for Microsoft Outlook Web Access is now downloadable via the FortiAuthenticator GUI as per the Microsoft Windows Agent



Windows FAC agent - group/OU exemptions

In order to accommodate the scenario where only a limited group of users are required to log into the Microsoft domain with two-factor authentication the ability to exempt users from two-factor auth using AD container filtering has been added to the FortiAuthenticator Agent for Microsoft Windows. Users who are members of an exempt groups and the users located under an exempt AD container are only required to provide a password to authenticate, i.e. no FortiToken code.

In order to improve user experience, group membership status of users is cached to support the scenario the workstation temporarily loses the ability to obtain the group membership information from the Windows AD server after having recently done a successful login, e.g. a user laptop home to work in the evening.



API

The REST API allows programmatic access to the FortiAuthenticator for integration with third party applications and business processes.

REST API - Set user expiration

User account expiration can now be set and modified via the API. See the REST API Guide for more details. http://docs.fortinet.com/fortiauthenticator/